

# Lexis 360®

## CONDITIONS D'AUTHENTIFICATION LEXISNEXIS 2019

# TABLE DES MATIERES

<b>MODIFICATIONS DES MODES D'ACCES AUX SERVICES AU COURS DE L'ANNEE 2019 .....</b>	<b>3</b>
<b>LE TRAITEMENT DES DONNEES A CARACTERE PERSONNEL.....</b>	<b>4</b>
<b>CONDITIONS D'AUTHENTIFICATION AUX SERVICES LEXISNEXIS.....</b>	<b>5</b>
ACCES PAR CODE ET MOT DE PASSE .....	5
AUTHENTIFICATION PAR RECONNAISSANCE IP ET LOGIN ET MOT DE PASSE .....	5
AUTHENTIFICATION AVEC LE PROTOCOLE SAML (SECURITY ASSERTION MARKUP LANGUAGE) .....	6
SHIBBOLETH (PRINCIPALEMENT POUR LES UNIVERSITES) .....	7
<b>CONDITIONS PARTICULIERES RELATIVES AUX ACCES .....</b>	<b>8</b>
<b>ANNEXES TECHNIQUES .....</b>	<b>9</b>
ANNEXE TECHNIQUE : AUTHENTIFICATION PAR CODE ET MOT DE PASSE .....	9
ANNEXE TECHNIQUE : AUTHENTIFICATION PAR ADRESSE IP.....	10
ANNEXE TECHNIQUE : AUTHENTIFICATION AVEC LE PROTOCOLE SAML (SECURITY ASSERTION MARKUP LANGUAGE) .....	11
ANNEXE TECHNIQUE : AUTHENTIFICATION PAR SHIBBOLETH.....	12

# Modifications des modes d'accès aux Services au cours de l'année 2019

En application du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 ainsi que de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifié par la loi n° 2018-493 du 20 juin 2018, LexisNexis en sa qualité de responsable du traitement renforce au cours de l'année 2019 les mesures techniques de connexion à ses différents Services afin de garantir un niveau de sécurité adapté pour chaque utilisateur assurant la confidentialité, l'intégrité, et la résilience constantes des données personnelles de chaque utilisateur.

Ces modifications permettront ainsi à l'Abonné de ne transmettre à LexisNexis que les seules

informations et données personnelles strictement nécessaires pour accéder aux Services. Elles vous garantissent auprès de vos propres utilisateurs une conformité obligatoire audit Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

Les principales modifications qui interviendront selon votre type d'accès sont décrites dans une annexe technique répertoriant les prérequis techniques.

Votre service client ainsi que votre interlocuteur commercial vous informera en amont de la date effective de la modification d'accès à votre abonnement.

ACTUELLEMENT	IMPACTS UTILISATEURS	IMPACTS ORGANISATION INFORMATIQUE
AUTHENTIFICATION PAR CODE ET MOT DE PASSE	Si le mot de passe n'est pas jugé assez sécurisé, certains utilisateurs préexistants pourront devoir changer de mot de passe une fois à la 1 <sup>ère</sup> connexion intervenant après la modification d'accès	Pas d'implication technique des services informatiques.
AUTHENTIFICATION PAR ADRESSE IP	Création d'un code d'accès et d'un mot de passe par chaque utilisateur, avec la possibilité de les enregistrer à la 1 <sup>ère</sup> connexion	-
AUTHENTIFICATION PAR INSTANT ACTIVATION	Selon le choix du Client, l'utilisateur accèdera désormais soit : <ul style="list-style-type: none"> <li>- Par l'un des 2 types d'accès ci-dessus (code et mot de passe ou adresse IP)</li> <li>- Par le protocole SAML</li> </ul>	Nécessité de choisir l'un des 3 modes d'accès : <ul style="list-style-type: none"> <li>- Par code et mot de passe</li> <li>- Par adresse IP</li> <li>- Par protocole SAML</li> </ul> Voir annexes techniques correspondants
AUTHENTIFICATION PAR SHIBBOLETH	Le raccourci vers l'écran d'authentification devra être changé par l'utilisateur une fois suivant la modification d'accès	Les services informatiques devront modifier l'accès au Service Provider

# Le traitement des données à caractère personnel

Les informations recueillies font l'objet d'un traitement informatique destiné notamment à gérer la relation commerciale dans le cadre de la fourniture de tous produits, abonnements et prestations de services, la prospection et l'élaboration de statistiques sur la base des données d'usage des Services et pour d'autres finalités complémentaires conformément à la Politique de confidentialité – données personnelles

<https://www.lexisnexis.fr/politique-confidentialite>. Les types d'informations recueillies sont : les coordonnées personnelles, les informations d'identification du compte, les données bancaires, tout commentaire ou information soumis et les coordonnées professionnelles. Les destinataires des données sont le personnel habilité du service marketing, du service commercial, des services chargés de traiter la relation client et la prospection, des services administratifs, des services logistiques et informatiques ainsi que leurs responsables hiérarchiques ; le personnel habilité des services chargés du contrôle au sein de LexisNexis SA, le Client, nos partenaires, nos filiales et nos éventuels sous-traitants dans le respect de la réglementation française et conformément à la Politique de confidentialité. Ces informations sont susceptibles de transfert hors du territoire de l'Espace économique européen mais bénéficient des garanties appropriées (Privacy Shield ou Clauses Contractuelles Types approuvées par la Commission Européenne). Sur demande, L'Editeur fournit au Client des données et analyses concernant l'utilisation des documents et des Services en ligne par les utilisateurs (ci-après les « Analyses »). Ces analyses

identifieront les différents niveaux d'usage Les données sont conservées pendant le délai strictement nécessaire à l'accomplissement des finalités susvisées conformément à la Politique de Confidentialité – données personnelles. L'Editeur fournira les Analyses au Client, à la condition impérative que ce dernier ne les utilise en aucun cas à des fins autres que le soutien des processus décisionnels internes, le contrôle de l'utilisation des documents et des Services en ligne, les activités que le Client mène avec l'Editeur en matière d'adoption de produits, ainsi que l'évaluation des niveaux d'utilisation et que les données des Analyses ne soient pas communiquées à des tiers sans avoir obtenu l'accord écrit préalable de l'Editeur. Le Client assume la responsabilité exclusive de la transmission et de l'obtention de tous consentements et autorisations nécessaires de la part des utilisateurs au regard de toutes les utilisations des Analyses et de l'accès aux Services fournis par l'Editeur.

Conformément à la réglementation applicable en matière de protection des données personnelles, toute personne dispose des droits (i) d'accès, (ii) de rectification, (iii) d'effacement, (iv) de limitation, (v) de portabilité des données et (vi) d'opposition au traitement en s'adressant via le portail Centre de Confidentialité (<https://www.lexisnexis.com/global/privacy/fr/privacy-centre-Inf.page>), au DPO [dpo@lexisnexis.co.uk](mailto:dpo@lexisnexis.co.uk) ou bien à l'adresse suivante [vosdonnees@lexisnexis.fr](mailto:vosdonnees@lexisnexis.fr), sous réserve le cas échéant de la justification de l'identité de la personne.

# Conditions d'authentification aux Services LexisNexis

Après acceptation du contrat souscrit par le Client, l'Editeur peut autoriser l'accès aux Services par différents modes, en fonction des Services souscrits par l'Abonné et des

caractéristiques techniques de son installation. Seul l'Editeur a la capacité de déterminer les modes d'accès qu'il souhaite donner à l'Abonné.

5

## Accès par code et mot de passe

Les codes d'accès aux Services et mots de passe sont personnels, confidentiels et intransmissibles. Ils sont exclusivement réservés à l'usage des utilisateurs nommément désignés. Ils ne peuvent, de quelque manière que ce soit, être communiqués à des tiers ou réutilisés, chez l'Abonné ou non, par une personne autre que l'utilisateur désigné. Le cas échéant, l'Editeur peut paramétrer les modalités d'accès par code et mot de passe : à cet effet lors de la première connexion, l'Editeur indiquera les différentes règles de saisie de ces éléments. L'Abonné doit notifier dans les meilleurs délais par mail ([relation.client@lexisnexis.fr](mailto:relation.client@lexisnexis.fr)) ou par courrier à

l'Editeur tout départ ou changement d'utilisateur, afin de faire procéder à l'annulation ou au remplacement des code et mot de passe. De même l'Abonné doit notifier toute perte ou vol d'identifiants à l'Editeur pour en permettre l'annulation. Pour des raisons de sécurité renforcée, l'éditeur peut décider d'une expiration des mots de passe tous les 6 mois : l'Editeur adresse lors de l'expiration un nouveau mot de passe pour une nouvelle durée de validité de 6 mois.

Le détail des évolutions et des prérequis techniques figure en annexe.

## Authentification par reconnaissance IP et login et mot de passe

L'accès aux Services par adressage IP, lorsqu'il est prévu, est exclusivement réservé à l'usage de l'Abonné et de ses collaborateurs via le réseau informatique ainsi identifié. Il ne peut, de quelque manière que ce soit, être partagé, étendu ou transmis à des utilisateurs, entités ou équipements informatiques n'appartenant pas à l'Abonné. La mise en œuvre de la reconnaissance IP est soumise au respect d'une procédure technique où l'Abonné s'oblige à communiquer à l'éditeur dans une annexe dédiée une description de son architecture informatique (architecture réseau, type de connexion Internet et matériel, adresses IP

publique des équipements et nombre d'utilisateurs experts associés). L'accès au Service ne peut se faire que depuis l'adresse IP définie, où chaque utilisateur s'authentifiera ensuite par un code et mot de passe personnel, confidentiel et intransmissible. Ces identifiants sont exclusivement réservés à l'usage des utilisateurs nommément désignés. Ils ne peuvent, de quelque manière que ce soit, être communiqués à des tiers ou réutilisés, chez l'Abonné ou non, par une personne autre que l'utilisateur désigné.

Les modalités d'accès par code et mot de passe seront à paramétrer : à cet effet lors de la première connexion, l'Editeur indiquera via un formulaire de création des identifiants les différentes règles de saisie de ces éléments. L'utilisateur devra par ailleurs définir une question secrète et la réponse correspondante, ainsi que les options de localisation. L'utilisateur aura la possibilité d'enregistrer ses identifiants par la fonction « Remember Me » pour ses prochaines connexions au Service.

Tout changement dans les modalités d'accès par adressage IP ou dans les caractéristiques du

réseau de l'Abonné utilisant cet adressage (cf nombre de d'utilisateurs experts connectés, localisation géographique des postes des utilisateurs experts, possibilité d'accès au réseau par des personnes tierces) est soumis à expertise préalable par l'Editeur, à qui l'Abonné doit le notifier par mail ([relation.client@lexisnexis.fr](mailto:relation.client@lexisnexis.fr)) ou par courrier dans les meilleurs délais, le cas échéant en complétant un document technique adressé par l'Editeur.

Le détail des évolutions et des prérequis techniques figure en annexe.

## Authentification avec le Protocole SAML (Security Assertion Markup Language)

L'accès aux Services par le mode d'authentification « Protocole SAML », lorsqu'il est prévu, est exclusivement réservé à l'usage de l'Abonné et de ses collaborateurs via le réseau informatique ainsi identifié. Il ne peut, de quelque manière que ce soit, être partagé, étendu ou transmis à des utilisateurs, entités ou équipements informatiques n'appartenant pas à l'Abonné. La mise en œuvre du protocole SAML est soumise au respect d'une norme (SAML 2.0) et d'une procédure technique où l'Abonné s'oblige à communiquer à l'éditeur dans une annexe dédiée une description de son architecture informatique (métadonnées de son serveur fournisseur d'identité [Identity Provider], un tableau de correspondance des attributs utilisateurs : Nom, Prénom, e-mail et code d'accès, ainsi que les éléments de personnalisation de chaque utilisateur). Il s'oblige également à prendre connaissance du Questionnaire des prérequis que lui remet l'éditeur

Ce mode d'authentification permet par ailleurs la gestion directement par l'Abonné de l'administration des comptes utilisateurs. Les informations et données personnelles des utilisateurs ne seront transmises à l'Editeur qu'au travers d'un échange SAML. Dans cette transmission, l'Editeur n'aura accès qu'aux seules informations et données personnelles strictement nécessaires.

L'Abonné autorise et accepte que l'Editeur puisse se connecter à l'annuaire mail de l'Abonné pour valider l'accès (au travers de l'échange avec l'Identity Provider Client) : cette modalité fera l'objet d'une mise en place convenue d'un commun accord avec l'Abonné.

Le détail des évolutions et des prérequis techniques figure en annexe.

## Shibboleth (principalement pour les Universités)

Pour les Abonnés, et sur décision uniquement de l'Editeur, ce dernier peut permettre l'accès et l'authentification aux Services via un processus dit de « délégation d'authentification » ou « Shibboleth ».

L'utilisateur pourra se connecter aux Services au moyen de codes et mots de passes personnels, confidentiels et intransmissibles, et utilisables uniquement dans un cadre universitaire attribués par son université.

Il ne peut, de quelque manière que ce soit, être partagé, étendu ou transmis à des utilisateurs, entités ou équipements informatiques n'appartenant pas à l'Abonné. La mise en œuvre du protocole Shibboleth est soumise au respect d'une norme (SAML 2.0) et d'une procédure technique où l'Abonné s'oblige à communiquer à l'éditeur dans une annexe dédiée une description de son architecture informatique (métadonnées de son serveur fournisseur d'identité [Identity Provider], un tableau de correspondance des attributs utilisateurs : Nom, Prénom, e-mail et code d'accès, ainsi que les éléments de personnalisation de chaque utilisateur).

Elle effectuera la modification du fichier de métadonnées du serveur d'identité en utilisant les éléments fournis par l'éditeur et/ou par RENATER (principalement : l'identifiant du serveur fournisseur d'identité, l'adresse informatique de déconnexion).

Pour les universités, l'utilisateur sera invité à sélectionner le serveur d'identité auquel il appartient, au moyen d'un outil « WAYF » (« Where Are You From »). La gestion des profils permet également de gérer les exclusions, afin de limiter les accès aux seuls profils autorisés.

Ce mode d'authentification permet par ailleurs la gestion directement par l'Abonné de l'administration des comptes utilisateurs et de leurs attributs. Les informations et données personnelles des utilisateurs ne seront transmises à l'Editeur qu'au travers d'un échange Shibboleth. Dans cette transmission, l'Editeur n'aura accès qu'aux seules informations et données personnelles strictement nécessaires.

L'Abonné autorise et accepte que l'Editeur puisse se connecter à l'annuaire mail de l'Abonné pour valider l'accès (au travers de l'échange avec l'Identity Provider Client) : cette modalité fera l'objet d'une mise en place convenue d'un commun accord avec l'Abonné.

Pour les modalités de mise en œuvre, nous invitons les universités à se rapprocher de l'Editeur.

Le détail des évolutions et des prérequis techniques figure en annexe.

# Conditions particulières relatives aux accès

L'Abonné admet que la connexion aux services peut être restreinte par l'éditeur qui se réserve la faculté de bloquer, pour des raisons légitimes et objectives, l'accès à son site internet provenant de terminaux identifiés.

En cas de contestation de l'Abonné écrite et motivée par des raisons objectives, l'éditeur rétablira la connexion aux services, à partir

dudit terminal. Sa responsabilité ne pourra d'aucune manière être recherchée pour le temps ou l'accès aux services aura été interrompu.

L'Abonné est seul responsable des accès aux services et toute utilisation qui en est faite avant modification ou annulation des moyens d'accès reste à la charge de l'Abonné.

# ANNEXES TECHNIQUES

## ANNEXE TECHNIQUE : Authentification par code et mot de passe

9

### Evolutions pour l'utilisateur

- L'utilisateur peut personnaliser son code utilisateur en respectant les règles suivantes :
  - o **doit** contenir 8 à 50 caractères
  - o **ne doit pas** contenir d'espace
  - o **peut** contenir les caractères spéciaux suivants : ! \$ & ' - ? ^ \_ ` { } ~ . @
- Le mot de passe doit respecter les règles suivantes :
  - o Doit contenir 8 à 50 caractères sans espace
  - o Ne doit pas contenir le code utilisateur ni l'un des 5 mots de passe précédents
  - o Doit contenir au minimum un caractère parmi 3 des catégories suivantes :
    - 1. Lettres majuscules (A-Z)
    - 2. Lettres minuscules (a-z)
    - 3. Chiffres (0-9)
    - 4. Caractères spéciaux : ! # \$ % & ' \* + - / = ? ^ \_ ` { | } ~ . @
- Les options de personnalisation sont conservées

### Evolutions pour l'administrateur client

- Si le client est précédemment équipé de CAT (Customer Admin Tool) :
  - o Une nouvelle interface d'administration est disponible
  - o Elle permet l'accès aux rapports d'usage
  - o Elle permet des modifications dans la gestion complète des préférences
  - o Le détail des fonctionnalités est disponible dans le manuel utilisateur de la nouvelle interface
- Pas d'évolution sinon

### Prérequis techniques

- Pour les clients utilisant des proxys type « EZ-PROXY » ou « Bibliopam »
  - o Nécessité pour les Services Informatiques du client de :
    - (Re)configurer les ressources accessibles par proxy à partir des nouveaux end-points et URL fournis par LexisNexis
    - S'assurer que EZ-PROXY et Bibliopam s'équipent de certificats SSL WildCard
- Aucun autre prérequis

### Planning de migration

- Au fil de l'eau, entre mars 2019 et juillet 2019

## ANNEXE TECHNIQUE : Authentification par Adresse IP

### Evolutions pour l'utilisateur

- A la modification d'accès, l'utilisateur crée son compte via un formulaire Nom + Prénom + e-mail (sous réserve qu'il accède au service via la plage d'adresse IP déclarée au préalable par les Services Informatiques du Client). Il crée son code d'accès, son mot de passe, sa question secrète et la réponse correspondante, ainsi que les options de localisation (langue).
- L'utilisateur peut personnaliser son code utilisateur en respectant les règles suivantes :
  - o **doit** contenir 8 à 50 caractères
  - o **ne doit pas** contenir d'espace
  - o **peut** contenir les caractères spéciaux suivants : ! \$ % & ' - ? ^ \_ ` { | } ~ . @
- Le mot de passe doit respecter les règles suivantes :
  - o Doit contenir 8 à 50 caractères sans espace
  - o Ne doit pas contenir le code utilisateur ni l'un des 5 mots de passe précédents
  - o Doit contenir au minimum un caractère parmi 3 des catégories suivantes :
    - 1. Lettres majuscules (A-Z)
    - 2. Lettres minuscules (a-z)
    - 3. Chiffres (0-9)
    - 4. Caractères spéciaux : ! # \$ % & ' \* + - / = ? ^ \_ ` { | } ~ . @
- Au prochain accès au produit, l'utilisateur est automatiquement reconnu sans saisie du login/mot de passe s'il a coché la case « Remember me » au moment de la création de son compte
- Les options de personnalisation sont conservées

### Evolutions pour l'administrateur client

- Si le client est précédemment équipé de CAT (Customer Admin Tool) :
  - o Une nouvelle interface d'administration est disponible
  - o Elle permet l'accès aux rapports d'usage
  - o Elle permet des modifications dans la gestion complète des préférences
  - o Le détail des fonctionnalités est disponible dans le manuel utilisateur de la nouvelle interface
- Pas d'évolution sinon

### Prérequis techniques

- Les Services Informatiques du Client confirment à LexisNexis :
  - o La plage d'adresses IP autorisées d'où les utilisateurs pourront se connecter au produit
  - o Les contraintes de domaine e-mail
  - o Le nombre maximum d'utilisateurs activables par IP
- Pour les clients utilisant des proxys type « EZ-PROXY » ou « Bibliopam »
  - o Nécessité pour les Services Informatiques du client de :
    - (Re)configurer les ressources accessibles par proxy à partir des nouveaux end-points et URL fournis par LexisNexis
    - S'assurer que EZ-PROXY et Bibliopam s'équipent de certificats SSL WildCard

## Planning de migration

- Entre avril 2019 et juin 2019, au fil de l'eau

# ANNEXE TECHNIQUE : Authentification avec le Protocole SAML (Security Assertion Markup Language)

11

## Evolutions pour l'utilisateur

- Nécessité d'authentifier l'utilisateur au sein de son serveur fournisseur d'identité

## Evolutions pour l'administrateur client :

- Si le client est précédemment équipé de CAT (Customer Admin Tool) :
  - o Une nouvelle interface d'administration est disponible
  - o Elle permet l'accès aux rapports d'usage
  - o Elle permet des modifications dans la gestion complète des préférences
  - o Le détail des fonctionnalités est disponible dans le manuel utilisateur de la nouvelle interface
- Pas d'évolution sinon

## Prérequis techniques

- Le client doit :
  - o Prendre connaissance du questionnaire de prérequis fourni par LexisNexis
  - o Déclarer le Service Provider LexisNexis au sein de l'Identity Provider en utilisant les métadonnées fournies par LexisNexis
  - o Fournir les métadonnées de son Serveur d'Identité (ID Provider)
  - o Etablir, en liaison avec LexisNexis, le tableau de correspondance (« mapping ») des attributs utilisateurs (Nom, prénom, e-mail, code d'accès).
- Si on souhaite récupérer des options de personnalisation actuelle, il faut définir une règle permettant de rétablir la correspondance du nouvel utilisateur avec les données existantes – sous réserve de faisabilité technique

Ces valeurs (Nom, Prénom, e-mail) sont obligatoires, l'adresse e-mail étant utilisée pour transmettre les paramètres de connexion.

## Planning de migration

- Entre février 2019 et juillet 2019

# ANNEXE TECHNIQUE : Authentification par Shibboleth

## Evolutions pour l'utilisateur

- L'utilisateur, à la modification d'accès, devra changer l'URL permettant l'accès et la redirection à nos services.

## Evolutions pour l'administrateur client

- Si le client est équipé de CAT (Customer Admin Tool) :
  - o Une nouvelle interface d'administration est disponible
  - o Elle permet l'accès aux rapports d'usage
  - o Elle permet des modifications dans la gestion complète des préférences
  - o Le détail des fonctionnalités est disponible dans le manuel utilisateur de la nouvelle interface
- Pas d'évolution sinon

12

## Prérequis techniques

- Côté LexisNexis
  - o L'adresse du serveur d'identité (IDP) associée au client université migré, est déclarée au sein du Service Provider (SP) de LexisNexis (Métadonnées IDP récupérées de RENATER dans le système).
- Côté Client
  - o Déclaration du nouveau SP au sein de son IDP par la modification du fichier de métadonnées de l'IDP en utilisant les métadonnées SP fournies par LexisNexis et/ou RENATER, principalement :
    - L'identifiant du serveur SP identity ID
    - Assertion (Tableau de correspondance (« Mapping ») (LexisNexis/IDP) des attributs utilisateurs à transmettre à notre SP)
    - URL de déconnexion (log out)
- Pour les clients utilisant des proxys type « EZ-PROXY » ou « Bibliopam »
  - o Nécessité pour les Services Informatiques du client de :
    - (Re)configurer les ressources accessibles par proxy à partir des nouveaux end-points et URL fournis par LexisNexis
    - S'assurer que EZ-PROXY et Bibliopam s'équipent de certificats SSL WildCard
- Si on souhaite récupérer des options de personnalisation actuelle, il faut définir une règle permettant de rétablir la correspondance du nouvel utilisateur avec les données existantes – sous réserve de faisabilité technique

## Planning de migration

- En mars 2019